REMARKS

Claims 1, 5 and 9 have been amended.

The Examiner has rejected claims 1-3, 5 and 7-8 under 35 U.S.C. 101 as being directed to non-statutory subject matter. Specifically, the Examiner states that based on the applicants' remarks submitted on 5/11/09 and based on what is disclosed in the specification the elements "an alteration unit" and "a control unit" as recited in claim 1 are software units per se. Applicants have amended claim 1 to replace the elements "an alteration unit" and "a control unit" with "a controller" and "a memory controller," respectively, which, as described in the specification, are physical structures that perform the functions of the replaced elements. Applicants believes that amended claim 1 is directed to statutory subject matter and that the Examiner's rejection under 35 U.S.C. 101 has been overcome.

The Examiner has rejected claims 1, 5, 9, 13 and 17 under 35 U.S.C. 102(b) as being anticipated by Ibaraki et al. ("Ibaraki") (US Patent 6,434,538). The Examiner has rejected claims 2-3, 7, 10-11 and 15 under 35 U.S.C. 103(a) as being unpatentable over Ibaraki. Lastly, the Examiner has rejected claims 8 and 16 under 35 U.S.C. 103(a) as being unpatentable over Ibaraki in view of Kondoh et al. ("Kondoh") (US Patent 6,968,058). Applicants have amended independent claims 1 and 9 and with respect to these claims, and their respective dependent claims, the Examiner's rejections are respectfully traversed.

Independent claim 1 has been amended to recite an image processing apparatus comprising: a controller that alters a first image file stored in a removable storage medium to generate a second image file, and a memory controller that stores the second image file in the storage medium, wherein the controller (a) controls the memory controller to store the second

image file in the storage medium without deleting the first image file from the storage medium, if the first image file includes authentication data that is used to authenticate whether the first image file has been altered, and (b) inquires whether to overwrite the second image file on the first image file stored in the storage medium, if the first image file does not include the authentication data. Independent claim 9 has been similarly amended.

The constructions recited in amended claim 1 and 9 are not taught or suggested in the cited art of record. More particularly, the Ibaraki and Kondoh references do not teach or suggest a controller (a) controlling the memory controller to store the second image file in the storage medium without deleting the first image file from the storage medium, if the first image file includes authentication data that is used to authenticate whether the first image file has been altered, and (b) inquires whether to overwrite the second image file on the first image file stored in the storage medium, if the first image file does not include the authentication data.

The Ibaraki reference is directed to a data control method for embedding and detecting data control information in data which is used to implement a copy control of the data. Abstract. As shown in Fig. 1A-1D, Ibaraki discloses copy control of the data in which copy prohibition information 31 is dispersed over an entire image 33 and permission information 32 is inserted in a predetermined position of the image 33 so that each permission information 32 permits the making of one copy (col. 6, lines 30-44). Ibaraki teaches that when copy prohibition information 31 alone is embedded over the image 33, copying of that image is prohibited altogether (col. 7, lines 1-6), and that when both copy prohibition information 31 and permission information 32 are embedded into the image 33, copying of that image is permitted once for each occurrence of the embedded permission information 32 (col. 7, lines 7-15). As shown in Fig. 3 of Ibaraki, permission information 32 is generated and embedded into the

image 33 as one or more occurrences of a digital signature f(m), with each occurrence of the digital signature f(m) allowing for a single copy of the image 33. In Fig. 5, Ibaraki discloses a method of detecting data control information by detecting and authenticating a digital signature f(m) representing permission information 32 within the image 33 (Step S5), so that authentication of the digital signature f(m) is an indication that the permission information 32 has been embedded in the image 33 (col. 11, lines 5-41). As shown in Fig. 4 of Ibaraki, if permission information 32 is detected in the image, then the process deletes at least a portion of the permission information 32 from the image 33 (Step S7) and sets a copy permission/prohibition flag to allow copying (Step S11) (col. 11, lines 44-54), and if permission information 32 is not detected, then detection of prohibition information 31 is performed (Step S8) (col. 11, lines 55-57) to determine whether or not copying is prohibited (Step S9). Ibaraki teaches that if prohibition information 31 is detected, then the copy/prohibition flag is set to prohibit copying (Step S10), and if prohibition information 31 is not detected, then the copy/prohibition flag is set to allow copying (Step S11) (col. 11, lines 59-65).

Therefore, Ibaraki discloses a data control method in which copying of the image is permitted when a digital signature within the image is authenticated or when the image is not embedded with prohibition information, and copying of the image is not permitted when the digital signature is not authenticated and the image is embedded with prohibition information. However, Ibaraki does not disclose the actual copying of the image file when the digital certificate is authenticated and makes no mention of any details concerning storage of the copied image file or overwriting the original image file. Rather, Ibaraki only discloses setting a copy permission/prohibition flag based on authentication of the digital signature and/or detection of prohibition information embedded in the image. Therefore, Ibaraki does not teach

or suggest altering a first image file stored in a removable storage medium to generate a second image file, storing the second image file in the storage medium and controlling whether or not to overwrite the first (original) image file.

Ibaraki is also completely silent as to controlling the storing of the second image file (copied image file) based on whether or not the first image file (original image file) includes authentication data that is used to authenticate whether the first image file has been altered. There is also no mention anywhere in Ibaraki of inquiring whether to overwrite the second image file on the first image file stored in the storage medium. Rather, Ibaraki only teaches controlling whether or not copying of the first image file is permitted in the first place, based on whether or not the first image file includes permission information and prohibition information embedded therein.

Accordingly, applicants' amended independent claims 1 and 9, each of which recite the controller (a) controlling the memory controller to store the second image file in the storage medium without deleting the first image file from the storage medium, if the first image file includes authentication data that is used to authenticate whether the first image file has been altered, and (b) inquires whether to overwrite the second image file on the first image file stored in the storage medium, if the first image file does not include the authentication data, and their respective dependent claims, patentably distinguish over the Ibaraki reference. Moreover, there is nothing added by the Kondoh reference to change this conclusion, and thus, applicants' amended independent claims 1 and 9, and their respective dependent claims, also patentably distinguish over the combination of the Ibaraki and Kondoh references.

In view of the above, it is submitted that applicants' claims, as amended, patentably distinguish over cited art of record. Accordingly, reconsideration and allowance of the application and claims is respectfully requested.

Dated: November 25, 2009

Respectfully submitted,

COWAN, LIEBOWITZ & LATMAN, P.C.
1133 Avenue of the Americas
New York, NY 10036-6799
T (212) 790-9200

John Laurence
Reg. No. 63,383